



(11) EP 4 451 604 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
23.10.2024 Bulletin 2024/43(51) International Patent Classification (IPC):
H04L 9/00 (2022.01) **H04L 9/06** (2006.01)(21) Application number: **24170357.8**(52) Cooperative Patent Classification (CPC):
H04L 9/003; H04L 9/0631; H04L 2209/122(22) Date of filing: **15.04.2024**

(84) Designated Contracting States:
**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB
GR HR HU IE IS IT LI LT LU LV MC ME MK MT NL
NO PL PT RO RS SE SI SK SM TR**
Designated Extension States:
BA
Designated Validation States:
GE KH MA MD TN

(30) Priority: **21.04.2023 KR 20230052904
20.06.2023 KR 20230078855**

(71) Applicant: **Samsung Electronics Co., Ltd.
Suwon-si, Gyeonggi-do 16677 (KR)**

(72) Inventors:

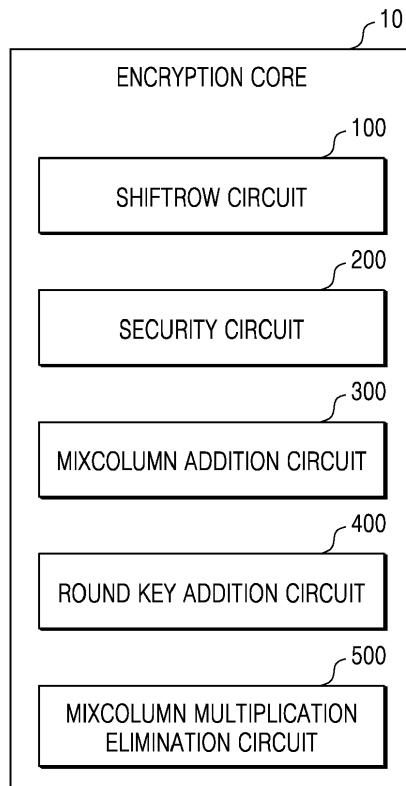
- **KIM, Gapkyoung**
16677 Suwon-si (KR)
- **KIM, Jaehyeok**
16677 Suwon-si (KR)
- **LEE, Yongki**
16677 Suwon-si (KR)
- **CHOI, Hongmook**
16677 Suwon-si (KR)

(74) Representative: **Marks & Clerk LLP
15 Fetter Lane
London EC4A 1BW (GB)**

(54) ENCRYPTION DEVICE AND OPERATING METHOD OF ENCRYPTION DEVICE

(57) An encryption device includes an encryption core circuit configured to generate output data by performing an encryption operation on input data, and an encryption controller circuit configured to control an operation of the encryption core. The encryption core circuit includes a shiftrow circuit configured to generate shift data by performing a shiftrow operation on the input data, a security circuit configured to generate permutation data by performing a permutation operation including a mix-column multiplication operation on the shift data, a mix-column addition circuit configured to generate first mid data by performing a mixcolumn addition operation on the permutation data, and a round key addition operation circuit configured to generate the output data by performing a round key addition operation on the first mid data.

FIG. 2



Description

TECHNICAL FIELD

5 [0001] Embodiments of the inventive concept relate to an encryption device that performs an encryption operation.

DISCUSSION OF RELATED ART

10 [0002] Smart cards and integrated circuit (IC) cards use secure information on users. In order to prevent security information of a user from being leaked by hacking, an encryption device that converts security information transmitted through a signature or authentication procedure into cipher text and transmits the cipher text may be utilized.

15 [0003] An attacker may attempt a side-channel analysis attack instead of directly manipulating input or output data. During the side-channel analysis attack, an attacker may collect additional information, such as the amount of power consumed by an encryption circuit and waveforms of an electromagnetic wave generated by an encryption device. An attacker may attack an encryption device to discover the key used by the encryption device based on the collected information.

SUMMARY

20 [0004] Embodiments of the inventive concept provides an encryption device that has high resistance to power analysis and may perform data encryption more quickly, and an operating method of the encryption device.

25 [0005] According to an aspect of the inventive concept, an encryption device includes an encryption core circuit configured to generate output data by performing an encryption operation on input data, and an encryption controller circuit configured to control an operation of the encryption core circuit. The encryption core circuit includes a shiftrow circuit configured to generate shift data by performing a shiftrow operation on the input data, a security circuit configured to generate permutation data by performing a permutation operation including a mixcolumn multiplication operation on the shift data, a mixcolumn addition circuit configured to generate first mid data by performing a mixcolumn addition operation on the permutation data, and a round key addition circuit configured to generate the output data by performing a round key addition operation on the first mid data.

30 [0006] The encryption operation may be a single round of an encryption algorithm. The input data may be the data input to and processed during that round. The input data may be the data output from a previous round. The output data generated by performing the encryption operation may be the output of the single round. The single round may comprise the shifting of the data, the generation of the permutation data, the generation of the first mid data, and the generation of the output data by performing the round key addition operation.

35 [0007] The controlling the operation of the encryption core circuit may comprise causing the encryption core circuit to perform the encryption operation on the input data. The encryption operation may comprise the shifting of the data, the generation of the permutation data, the generation of the first mid data, and the generation of the output data by performing the round key addition operation.

40 [0008] The security circuit may be configured to generate the permutation data by performing an operation to select one of a plurality of integers for each value of the shift data to obtain a selected integer corresponding to each of the values of the shift data. The plurality of integers may be selected from an S-box. The security circuit may be configured to first decode the shift data to obtain decoded values and use the decoded values to perform the selection of the integers for the shift data. The operation of selecting the ones of the plurality of integers may be a substitution operation. The permutation operation may comprise the substitution operation in combination with the mixcolumn multiplication operation. The mixcolumn multiplication operation may be performed on the selected integers. The permutation operation may be a T-box operation.

45 [0009] The first mid data may also be referred to as a first intermediate value. The encryption core circuit may further comprise a mixcolumn multiplication elimination circuit configured to generate second mid data. The second mid data may also be referred to as a second intermediate value.

50 [0010] The mixcolumn multiplication operation and mixcolumn addition operation may together constitute a mixcolumn operation. The mixcolumn operation may comprise performing a matrix multiplication between a matrix of data derived from the shift data and a predefined matrix. The mixcolumn multiplication operation may comprise the multiplication operations between elements of the matrices performed as part of the matrix multiplication. The mixcolumn addition operation may comprise the addition operations performed between values resulting from the multiplication operations to generate elements of the first mid data matrix. The matrix of data derived from the shift data may comprise a matrix comprising the selected ones of the plurality of integers selected based on the shift data.

55 [0011] The round key addition operation may comprise combining each bit of the first mid data with a round key using bitwise XOR operations. The round key may be derived for the particular round of the encryption algorithm from a cipher

key using a key schedule.

[0012] In some embodiments, the encryption data further comprises: a mixcolumn multiplication elimination circuit configured to generate second mid data by performing a mixcolumn multiplication elimination operation on the permutation data, wherein the round key addition operation circuit generates the output data by performing the round key addition operation on the second mid data. The mixcolumn multiplication elimination operation reverses the mixcolumn multiplication operation.

[0013] In some embodiments, the encryption core circuit is configured to generate ciphertext data by performing a plurality of round operations on plaintext data, and the encryption controller circuit is configured to control the encryption core circuit to sequentially perform the plurality of round operations including an initial round operation, an iterative round operation of a preset reference number of times, and a final round operation, wherein the iterative round operation includes the shiftrow operation, the permutation operation, the mixcolumn addition operation, and the round key addition operation. The final round operation may comprise a mixcolumn multiplication elimination operation in addition to the shiftrow operation, the permutation operation, and the round key addition operation. The mixcolumn multiplication elimination operation may reverse the mixcolumn multiplication operation. The mixcolumn multiplication elimination operation may be performed on the permutation data produced by the permutation operation to generate second mid data on which the round key addition operation is performed.

[0014] According to an aspect of the inventive concept, an encryption device includes an encryption core circuit configured to generate output data by performing a plurality of round operations on input data, and an encryption controller circuit configured to control the encryption core to sequentially perform a plurality of round operations including an initial round operation, an iterative round operation of a preset reference number of times, and a final round operation. The encryption core circuit includes a shiftrow circuit configured to generate shift data by performing a shiftrow operation on the input data, a security circuit configured to generate permutation data by performing a permutation operation including a mixcolumn multiplication operation on the shift data, a mixcolumn addition circuit configured to generate first mid data by performing a mixcolumn addition operation on the permutation data, and a round key addition operation circuit configured to generate the output data by performing a round key addition operation on the first mid data. The iterative round operation includes the shiftrow operation, the permutation operation, the mixcolumn addition operation, and the round key addition operation.

[0015] According to an aspect of the inventive concept, an operating method of an encryption device including an encryption core circuit configured to generate output data by performing an encryption operation on input data and an encryption controller circuit configured to control an operation of the encryption core, includes generating shift data by performing a shiftrow operation on the input data, generating permutation data by performing a permutation operation including a mixcolumn multiplication operation on the shift data, generating first mid data by performing a mixcolumn addition operation on the permutation data, and generating the output data by performing a round key addition operation on the first mid data.

[0016] At least some of the above and other features of the invention are set out in the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] The above and other features of the inventive concept will become more apparent by describing in detail embodiments thereof with reference to the accompanying drawings, in which:

- FIG. 1 is a block diagram illustrating an encryption device according to an embodiment;
- FIG. 2 is a block diagram illustrating an encryption core according to an embodiment;
- FIG. 3 is a block diagram illustrating a detailed configuration of a security circuit and an example of data input and output to and from the security circuit according to an embodiment;
- FIG. 4 is a block diagram illustrating an example in which a sub security circuit illustrated in FIG. 3 includes one encoder;
- FIG. 5 is a block diagram illustrating a detailed configuration of a security circuit and an example of data input and output to and from the security circuit according to an embodiment;
- FIG. 6 is a block diagram illustrating an example in which a sub security circuit illustrated in FIG. 5 includes a plurality of encoders;
- FIG. 7 is a block diagram illustrating an example in which a sub security circuit illustrated in FIG. 5 includes a plurality of encoders and a plurality of additional operation circuits;
- FIG. 8 is a table illustrating an example of a mixcolumn multiplication operation result that may be output through the plurality of encoders and the plurality of additional operation circuits in the sub security circuit of FIG. 7;
- FIG. 9 is a table illustrating an example of a mixcolumn multiplication operation result that may be output through the plurality of encoders and the plurality of additional operation circuits in the sub security circuit of FIG. 7;
- FIG. 10 is a table illustrating an example in which a mixcolumn multiplication operation result may be generated

through a configuration of a sub security circuit, according to an embodiment;

FIG. 11 is a table illustrating an example in which a mixcolumn multiplication operation result may be generated through a configuration of a sub security circuit, according to an embodiment;

FIG. 12 is a block diagram illustrating a detailed configuration of a mixcolumn addition circuit and an example of data input and output to and from a security circuit according to an embodiment;

FIG. 13 is a flowchart illustrating an operating method of an encryption device, according to an embodiment; and

FIG. 14 is a block diagram illustrating a computing device according to an embodiment.

DETAILED DESCRIPTION OF AN EMBODIMENT

[0018] Embodiments of the present disclosure will be described more fully hereinafter with reference to the accompanying drawings. Like reference numerals may refer to like elements throughout the accompanying drawings.

[0019] It will be understood that the terms "first," "second," "third," etc. are used herein to distinguish one element from another, and the elements are not limited by these terms. Thus, a "first" element in an embodiment may be described as a "second" element in another embodiment.

[0020] It should be understood that descriptions of features or aspects within each embodiment should typically be considered as available for other similar features or aspects in other embodiments, unless the context clearly indicates otherwise.

[0021] As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise.

FIG. 1 is a block diagram illustrating an encryption device according to an embodiment.

[0022] Referring to FIG. 1, an encryption device 1 according to an embodiment may include an encryption core 10 and an encryption controller 20. The encryption core 10 may also be referred to as an encryption core circuit, and the encryption controller 20 may also be referred to herein as an encryption controller circuit.

[0023] The encryption core 10 may generate output data by performing an encryption operation on input data.

[0024] The encryption core 10 may include various types of operation circuits. For example, the encryption core 10 may include various types of operation circuits, such as a shiftrow circuit, a security circuit, a mixcolumn addition circuit, a round key addition circuit, and a mixcolumn multiplication elimination circuit. The encryption core 10 may generate output data by performing an encryption operation on input data by performing operations through various types of operation circuits based on a control signal received from the encryption controller 20.

[0025] The encryption core 10 may generate output data by performing a plurality of round operations on input data. The plurality of round operations may include, for example, an initial round operation, an iterative round operation of a preset number of times, and a final round operation.

[0026] In an embodiment, the first round operation may include a round key addition operation performed by a round key addition operation circuit. The first round operation may be performed in a first operation of encryption on input data. An iterative round operation may be performed after the initial round operation is performed.

[0027] In an embodiment, the iterative round operation may include a shiftrow operation performed by a shiftrow circuit, a permutation operation performed by a security circuit, a mixcolumn addition operation performed by a mixcolumn addition circuit, and a round key addition operation performed by a round key addition operation circuit. The iterative round operation may be performed subsequent to a first round operation and may be performed as many as a preset reference number of times. The final round operation may be performed after the iterative round operation is performed as many as a reference number of times.

[0028] In an embodiment, the final round operation may include a shiftrow operation performed by a shiftrow circuit, a permutation operation performed by a security circuit, a mixcolumn multiplication elimination operation performed by a mixcolumn multiplication elimination circuit, and a round key addition operation performed by a round key addition operation circuit. By performing the final round operation, final output data in which input data is encrypted may be generated.

[0029] The encryption controller 20 may control all operations of the encryption device 1. The encryption controller 20 may control an operation of the encryption core 10 by transmitting a control signal to the encryption core 10.

[0030] The encryption controller 20 may control the encryption core 10 to sequentially perform the initial round operation, the iterative round operation of a preset reference number of times, and the final round operation.

[0031] FIG. 2 is a block diagram illustrating an encryption core according to an embodiment.

[0032] Referring to FIG. 2, the encryption core 10 according to an embodiment may include a shiftrow circuit 100, a security circuit 200, a mixcolumn addition circuit 300, a round key addition circuit 400, and a mixcolumn multiplication elimination circuit 500.

[0033] The shiftrow circuit 100 may perform a shiftrow operation on input data. The shiftrow circuit 100 may perform a shiftrow operation on input data by cyclically shifting rows of the input data in a cyclic structure.

[0034] The shiftrow operation may be represented by Equation 1 below.

[Equation 1]

$$\begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix} \rightarrow \begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_5 & x_9 & x_{13} & x_1 \\ x_{10} & x_{14} & x_2 & x_6 \\ x_{15} & x_3 & x_7 & x_{11} \end{bmatrix}$$

[0035] The shiftrow circuit 100 may generate shift data as a result of performing a shiftrow operation on input data.

The shift data generated by the shiftrow circuit 100 may be input to the security circuit 200 under control of the encryption controller 20.

[0036] The security circuit 200 may perform a permutation operation including a mixcolumn multiplication operation on the shift data.

[0037] The permutation operation may generate permutation data by performing nonlinear permutation on the shift data. In an embodiment, the permutation operation may be an operation for permutation on a result of performing a mixcolumn multiplication operation on a result of passing the received shift data through an S-Box. That is, in an embodiment, the permutation operation may be a permutation operation for passing through a T-box that permutes with a result of performing a mixcolumn multiplication operation on a result that the received shift data passes through the S-Box. In this case, the T-Box is similar to the S-Box but may be a box for permutation to reflect a result of performing a mixcolumn multiplication operation.

[0038] In this case, the mixcolumn operation may be a matrix multiplication operation between input data and a preset mixcolumn matrix. For example, for the sake of simplicity of description, a mixcolumn operation between a data matrix and a mixcolumn matrix, which are represented by a 2*2 matrix, may be represented by Equation 2 below.

[Equation 2]

$$D * M = \begin{bmatrix} D_1 & D_2 \\ D_3 & D_4 \end{bmatrix} * \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix} = \begin{bmatrix} D_1 * M_1 + D_2 * M_3 & D_1 * M_2 + D_2 * M_4 \\ D_3 * M_1 + D_4 * M_3 & D_3 * M_2 + D_4 * M_4 \end{bmatrix} = R$$

[0039] In Equation 2, a matrix D may be a data matrix, a matrix M may be a mixcolumn matrix, and a matrix R may be a mixcolumn operation result matrix. Each element of the mixcolumn operation result matrix R may be represented by the product and sum of elements of the data matrix D and the mixcolumn matrix M.

[0040] The mixcolumn operation may be divided into a mixcolumn multiplication operation and a mixcolumn sum operation. In this case, the mixcolumn multiplication operation may correspond to an operation for multiplying respective elements of matrices in a matrix multiplication operation, and the mixcolumn sum operation may correspond to a sum operation between results of multiplication between respective elements of matrices in a matrix multiplication operation.

[0041] For example, in (1,1) element of the mixcolumn operation result matrix R of Equation 2, D1*M1 and D2*M3 may be classified as a mixcolumn multiplication operation and the sum operation of the results of D1*M1 and D2*M3 may be classified as a mixcolumn sum operation.

[0042] That is, the security circuit 200 may perform a permutation operation of passing through a T-Box that permutes with a result of performing the mixcolumn multiplication operation described above on a result of passing the shift data through an S-Box.

[0043] The security circuit 200 may generate permutation data as a result of performing a permutation operation, which includes a mixcolumn multiplication operation, on the shift data. The permutation data generated by the security circuit 200 may be input to the mixcolumn addition circuit 300 or the mixcolumn multiplication elimination circuit 500 under control of the encryption controller 20.

[0044] A more detailed structure and an operation of the security circuit 200 are described below with reference to FIGS. 3 to 7.

[0045] The mixcolumn addition circuit 300 may perform a mixcolumn addition operation on the permutation data. The mixcolumn addition circuit 300 may perform a mixcolumn addition operation on the permutation data including to which the result of the mixcolumn multiplication operation generated by the security circuit 200 is also reflected. That is, the mixcolumn addition circuit 300 may complete the mixcolumn operation in which the mixcolumn multiplication operation is performed by the security circuit 200.

[0046] The mixcolumn addition circuit 300 may generate first mid data as a result of performing the mixcolumn addition operation on the permutation data. The first mid data generated by the mixcolumn addition circuit 300 may be input to the round key addition operation circuit 400 under control of the encryption controller 20.

[0047] A more detailed structure and an operation of the mixcolumn addition circuit 300 are described below with

reference to FIG. 12.

[0048] The round key addition operation circuit 400 may perform a round key addition operation on the first mid data. The round key addition operation circuit 400 may perform a round key addition operation by performing a bitwise combinatorial logic operation (for example, an exclusive OR operation (XOR)) between the first mid data and a round key.

[0049] The round key addition operation circuit 400 may generate output data as a result of performing the round key addition operation on the first mid data. The output data generated by the round key addition operation circuit 400 may be used in the next round operation under control of the encryption controller 20. For example, when the output data generated by the round key addition operation circuit 400 is generated in an initial round operation or an iterative round operation, the output data may be used in a next iterative round operation or a final round operation.

[0050] The round key addition operation circuit 400 may generate output data by performing a round key addition operation on a second mid data generated by the mixcolumn multiplication elimination circuit 500 to be described below.

[0051] The output data generated by performing the round key addition operation on the second mid data by the round key addition operation circuit 400 may be used as final output data. For example, when the output data generated by the round key addition operation circuit 400 is generated in the final round operation, the output data may be used as final output data obtained by encrypting the input data.

[0052] The mix-column multiplication elimination circuit 500 may perform a mix-column multiplication elimination operation on permutation data. The mixcolumn multiplication elimination circuit 500 may perform an operation of converting the permutation data, to which a result of the mixcolumn multiplication operation generated by the security circuit 200 is reflected, into data on which the mixcolumn multiplication operation is not performed. That is, the mixcolumn multiplication elimination circuit 500 may convert data on which the mixcolumn multiplication operation is performed into data on which the mixcolumn multiplication operation is not performed.

[0053] In this way, the encryption core 10 does not include an additional security circuit that generates permutation data as a result of performing a permutation operation, which does not include a mixcolumn multiplication operation, on shift data, separately from the security circuit 200, and includes a mixcolumn multiplication elimination circuit 500, and thus, an increase in the area occupied by the encryption core 10 may be greatly reduced. The encryption core 10 may also be referred to as a cryptographic core.

[0054] The mixcolumn multiplication elimination circuit 500 may generate the second mid data as a result of performing a mixcolumn multiplication elimination operation on the permutation data. The second mid data generated by the mix-column multiplication elimination circuit 500 may be input to the round key addition operation circuit 400 under control of the encryption controller 20.

[0055] As described above, when the encryption device 1 according to an embodiment of the inventive concept is used, permutation data may be generated by performing a permutation operation including a mixcolumn multiplication operation on shift data by the security circuit 200, and thus, a critical path may be reduced.

[0056] FIG. 3 is a block diagram illustrating a detailed configuration of a security circuit and an example of data input and output to and from the security circuit according to an embodiment.

[0057] Referring to FIG. 3, in an embodiment, the security circuit 200 may receive shift data SD.

[0058] The shift data SD may be divided into first to fourth sub shift data SSD1 to SSD4. The first to fourth sub shift data SSD1 to SSD4 are data generated by dividing the shift data SD into data having the same size, and may become the shift data SD by connecting the first to fourth sub shift data SSD1 to SSD4 to each other. In an embodiment of FIG. 3, the shift data SD includes 32 bits total, and the shift data SD may be divided into 4 pieces. In this case, the first sub shift data SSD1 may include the most significant 8 bits of the shift data SD, the second sub shift data SSD2 may include upper 8 bits following the first sub shift data SSD1, the third sub shift data SSD3 may include upper 8 bits following the second sub shift data SSD2, and the fourth sub shift data SSD4 may include the least significant 8 bits of the shift data SD.

[0059] In an embodiment of FIG. 3, the security circuit 200 may include first to twelfth sub security circuits 210_1 to 210_12.

[0060] In an embodiment of FIG. 3, the number of security circuits (for example, the first to twelfth sub security circuits 210_1 to 210_12) may be equal to the number obtained by multiplying the number of pieces of sub shift data (for example, the first to fourth sub shift data SSD1 to SSD4) by the number of mixcolumn multiplication values.

[0061] In an embodiment, a mixcolumn matrix used for encryption of input data may be represented by Equation 3 below.

[Equation 3]

$$\begin{bmatrix} \{02\} & \{03\} & \{01\} & \{01\} \\ \{01\} & \{02\} & \{03\} & \{01\} \\ \{01\} & \{01\} & \{02\} & \{03\} \\ \{03\} & \{01\} & \{01\} & \{02\} \end{bmatrix}$$

[0062] In this case, three values, such as {01}, {02}, and {03}, which are element values of the mixcolumn matrix, may be referred to as the mixcolumn multiplication values. In an embodiment of FIG. 3, when the number of pieces of sub shift data (for example, the first to fourth sub shift data SSD1 to SSD4) is 4 and the number of mixcolumns multiplication values is 3 as illustrated in Equation 3, the number of sub security circuits (for example, the first to twelfth sub security circuits 210_1 to 210_12) may be 12 in total.

[0063] Each of the first to twelfth sub security circuits 210_1 to 210_12 may receive any one of the first to fourth sub shift data SSD1 to SSD4 generated by dividing the shift data SD.

[0064] In an embodiment of FIG. 3, the first to third sub security circuits 210_1 to 210_3 may receive the first sub shift data SSD1, the fourth to sixth sub security circuits 210_4 to 210_6 may receive the second sub shift data SSD2, the seventh to ninth sub security circuits 210_7 to 210_9 may receive the third sub shift data SSD3, and the tenth to twelfth sub security circuits 210_10 to 210_12 may receive the fourth sub shift data SSD4.

[0065] Each of the first to twelfth sub security circuits 210_1 to 210_12 may perform a permutation operation, which includes a mixcolumn multiplication operation on any one of a plurality of mixcolumn multiplication values, on the received sub shift data. Each of the first to twelfth sub security circuits 210_1 to 210_12 may generate any one of first to third multiplication data MD1 to MD3 included in first to fourth sub permutation data SSuD1 to SSuD4 by performing a permutation operation.

[0066] In an embodiment of FIG. 3, permutation data SuD may include the first to fourth sub permutation data SSuD1 to SSuD4. The permutation data SuD may have a form in which the first to fourth sub permutation data SSuD1 to SSuD4 are sequentially connected to each other. In this case, each of the first to fourth sub permutation data SSuD1 to SSuD4 may include the first to third multiplication data MD1 to MD3. Each of the first to fourth sub permutation data SSuD1 to SSuD4 may have a form in which the first to third multiplication data MD1 to MD3 are sequentially connected to each other.

[0067] In an embodiment of FIG. 3, the first sub security circuit 210_1 may perform a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {02}, on the first sub shift data SSD1. The first sub security circuit 210_1 may generate the first multiplication data MD1 included in the first sub permutation data SSuD1 as a result of the permutation operation.

[0068] In an embodiment of FIG. 3, the second sub security circuit 210_2 may perform a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {01}, on the first sub shift data SSD1. The second sub security circuit 210_2 may generate the second multiplication data MD2 included in the first sub permutation data SSuD1 as a result of the permutation operation.

[0069] In an embodiment of FIG. 3, the third sub security circuit 210_3 may perform a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {03}, on the first sub shift data SSD1. The third sub security circuit 210_3 may generate the third multiplication data MD3 included in the first sub permutation data SSuD1 as a result of the permutation operation.

[0070] In an embodiment of FIG. 3, the fourth sub security circuit 210_4 may generate the first multiplication data MD1 included in the second sub permutation data SSuD2 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {02}, on the second sub shift data SSD2. The fifth sub security circuit 210_5 may generate the second multiplication data MD2 included in the second sub permutation data SSuD2 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {01}, on the second sub shift data SSD2. The sixth sub security circuit 210_6 may generate the third multiplication data MD3 included in the second sub permutation data SSuD2 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {03}, on the second sub shift data SSD2.

[0071] In an embodiment of FIG. 3, the seventh sub security circuit 210_7 may generate the first multiplication data MD1 included in the third sub permutation data SSuD3 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {02}, on the third sub shift data SSD3. The eighth sub security circuit 210_8 may generate the second multiplication data MD2 included in the third sub permutation data SSuD3 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {01}, on the third sub shift data SSD3. The ninth sub security circuit 210_9 may generate the third multiplication data MD3 included in the third sub permutation data SSuD3 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {03}, on the third sub shift data SSD3.

[0072] In an embodiment of FIG. 3, the tenth sub security circuit 210_10 may generate the first multiplication data MD1 included in the fourth sub permutation data SSuD4 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {02}, on the fourth sub shift data SSD4. The eleventh sub security circuit 210_11 may generate the second multiplication data MD2 included in the fourth sub permutation data SSuD4 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {01}, on the fourth sub shift data SSD4. The twelfth sub security circuit 210_12 may generate the third multiplication data MD3 included in the fourth sub permutation data SSuD4 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {03}, on the fourth

sub shift data SSD4.

[0073] In this case, each of the first to twelfth sub security circuits 210_1 to 210_12 may receive sub shift data different from other sub security circuits or perform a permutation operation including a mixcolumn multiplication operation on different mixcolumn multiplication values. For example, the first sub security circuit 210_1 may receive the same sub shift data as the second sub security circuit 210_2 but may perform a permutation operation including a mixcolumn multiplication operation on different mixcolumn multiplication values. Also, the first sub security circuit 210_1 may perform a permutation operation including a mixcolumn multiplication operation on the same mixcolumn multiplication value as the fourth sub security circuit 210_4 but may receive different sub shift data.

[0074] A more detailed structure of the first to twelfth sub security circuits 210_1 to 210_12 is described with reference to FIG. 4.

[0075] FIG. 4 is a block diagram illustrating an example in which the sub security circuit illustrated in FIG. 3 includes one encoder.

[0076] Referring to FIG. 4, a first sub security circuit 210_1 according to an embodiment may include a decoder 211_1, a permutation circuit 212_1, and an encoder 213_1. The decoder 211_1 may also be referred to as a decoder circuit, and the encoder 213_1 may also be referred to as an encoder circuit. The second to twelfth sub security circuits 210_2 to 210_12 other than the first sub security circuit 210_1 may each also have the same structure as the first sub security circuit 210_1.

[0077] The decoder 211_1 may decode the received sub shift data and output a decoded value. In an embodiment, the decoder 211_1 may include a plurality of logic gates. The decoder 211_1 may receive sub shift data and inverted sub shift data through the plurality of logic gates. The decoder 211_1 may pass the received sub shift data and the inverted sub shift data through a plurality of logic gates, thereby decoding the received sub shift data and outputting a decoded value.

[0078] The permutation circuit 212_1 may output a selected permutation value based on the decoded value. In an embodiment, the permutation circuit 212_1 may select any one of a plurality of integers based on the decoded value and output the selected value as a permutation value.

[0079] The encoder 213_1 may generate multiplication data by encoding the permutation value to represent a result of a mixcolumn multiplication operation on any one of a plurality of mixcolumn multiplication values. In an embodiment, the encoder 213_1 may receive the permutation value through a plurality of logic gates. The encoder 213_1 may pass the permutation value through the plurality of logic gates, thereby encoding the permutation value to represent the result of the mixcolumn multiplication operation on any one of the plurality of mixcolumn multiplication values to generate the multiplication data.

[0080] In this way, when the security circuit 200 according to an embodiment of the inventive concept is used, the encoder 213_1 may perform encoding to represent a result of a mixcolumn multiplication operation, and accordingly, a critical path may be reduced.

[0081] FIG. 5 is a block diagram illustrating a detailed configuration of a security circuit and an example of data input and output to and from the security circuit according to an embodiment.

[0082] Referring to FIG. 5, in an embodiment, a security circuit 200 may receive shift data SD.

[0083] In an embodiment of FIG. 5, the security circuit 200 may include first to fourth sub security circuits 210_1 to 210_4.

[0084] In an embodiment of FIG. 5, the number of sub security circuits (for example, the first to fourth sub security circuits 210_1 to 210_4) may be equal to the number of pieces of sub shift data (for example, the first to fourth sub shift data SSD1 to SSD4).

[0085] Each of the first to fourth sub security circuits 210_1 to 210_4 may receive any one of the first to fourth sub shift data SSD1 to SSD4 generated by dividing the shift data SD. In this case, each of the first to fourth sub security circuits 210_1 to 210_4 may receive sub shift data different from sub shift data of other sub security circuits.

[0086] In an embodiment of FIG. 5, the first sub security circuit 210_1 may receive the first sub shift data SSD1, the second sub security circuit 210_2 may receive the second sub shift data SSD2, the third sub security circuit 210_3 may receive the third sub shift data SSD3, and the fourth sub security circuit 210_4 may receive the fourth sub shift data SSD4.

[0087] Each of the first to fourth sub security circuits 210_1 to 210_4 may perform a permutation operation including a mixcolumn multiplication operation on the sub shift data. The first to fourth sub security circuits 210_1 to 210_4 may generate first to fourth sub permutation data SSuD1 to SSuD4, each including first to third multiplication data MD1 to MD3, by performing permutation operations.

[0088] In an embodiment of FIG. 5, the first sub security circuit 210_1 may perform a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication values {02}, {01}, and {03}, on the first sub shift data SSD1. The first sub security circuit 210_1 may generate first sub permutation data SSuD1 including the first to third multiplication data MD1 to MD3 as a result of a permutation operation. In this case, the first sub security circuit 210_1 may generate the first multiplication data MD1 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {02}, on the first sub shift data SSD1. The first sub security circuit 210_1 may generate the second multiplication data MD2 by performing a permutation operation,

which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {01}, on the first sub shift data SSD1. The first sub security circuit 210_1 may generate the third multiplication data MD3 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication value {03}, on the first sub shift data SSD1.

[0089] In an embodiment of FIG. 5, the second sub security circuit 210_2 may generate the second sub permutation data SSuD2 including the first to third multiplication data MD1 to MD3 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication values {02}, {01}, and {03}, on the second sub shift data SSD2. The third sub security circuit 210_3 may generate the third sub permutation data SSuD3 including the first to third multiplication data MD1 to MD3 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication values {02}, {01}, and {03}, on the third sub shift data SSD3. The fourth sub security circuit 210_4 may generate the fourth sub permutation data SSuD4 including the first to third multiplication data MD1 to MD3 by performing a permutation operation, which includes a mixcolumn multiplication operation on the mixcolumn multiplication values {02}, {01}, and {03}, on the fourth sub shift data SSD4.

[0090] A more detailed structure of the first to fourth sub security circuits 210_1 to 210_4 is described with reference to FIG. 6.

[0091] FIG. 6 is a block diagram illustrating an example in which the sub security circuit illustrated in FIG. 5 includes a plurality of encoders.

[0092] Referring to FIG. 6, the first sub security circuit 210_1 according to an embodiment may include a decoder 211_1, a permutation circuit 212_1, a first encoder 213_1 1, a second encoder 213_12, and a third encoder 213_13. The second to fourth sub security circuits 210_2 to 210_4 other than the first sub security circuit 210_1 may each also have the same structure as the first sub security circuit 210_1.

[0093] The decoder 211_1 and the permutation circuit 212_1 may perform the same operations as described with reference to FIG. 4.

[0094] The first to third encoders 213_11 to 213_13 may perform the same operations as described with reference to FIG. 4.

[0095] In this case, the first to third encoders 213_11 to 213_13 may generate multiplication data by encoding a permutation value to represent a result of a mixcolumn multiplication operation on any one of a plurality of mixcolumn multiplication values. For example, the first encoder 213_11 may generate multiplication data by encoding a permutation value to represent a result of a mixcolumn multiplication operation on the mixcolumn multiplication value {02}. The second encoder 213_12 may generate multiplication data by encoding a permutation value to represent a result of a mixcolumn multiplication operation on the mixcolumn multiplication value {01}. The third encoder 213_13 may generate multiplication data by encoding a permutation value to represent a result of a mixcolumn multiplication operation on the mixcolumn multiplication value {03}.

[0096] In this way, when the security circuit 200 according to embodiments of FIGS. 5 and 6 is used, the first to third encoders 213_11 to 213_13 share the same decoder 211_1 and the permutation circuit 212_1, and thus, an increase in a total area of the security circuit 200 may be reduced.

[0097] As described above, although an encryption operation of the encryption device 1 is mainly described with reference to FIGS. 1 to 6, the same description may be applied to a decryption operation.

[0098] FIG. 7 is a block diagram illustrating an example in which the sub security circuit illustrated in FIG. 5 includes a plurality of encoders and a plurality of additional operation circuits.

[0099] Referring to FIG. 7, the first sub security circuit 210_1 according to an embodiment may include a decoder 211_1, a permutation circuit 212_1, a first encoder 213_1 1, a second encoder 213_12, a third encoder 213_13, a fourth encoder 213_14, a first additional operation circuit 214_11, a second additional operation circuit 214_12, and a third additional operation circuit 214_13. The second to fourth sub security circuits 210_2 to 210_4 other than the first sub security circuit 210_1 may each also have the same structure as the first sub security circuit 210_1.

[0100] The decoder 211_1 and the permutation circuit 212_1 may perform the same operations as described with reference to FIG. 4.

[0101] Although FIG. 6 illustrates an embodiment in which one sub security circuit includes three encoders, FIG. 6 mainly illustrates an encryption operation of the encryption device 1, and an additional encoder is utilized to enable the encryption device 1 to perform the decryption operation.

[0102] For example, a mixcolumn matrix used to decode input data may be represented by Equation 4 below.

[Equation 4]

$$\begin{bmatrix}
 \{0E\} & \{09\} & \{0B\} & \{0D\} \\
 \{0D\} & \{0E\} & \{09\} & \{0B\} \\
 \{0B\} & \{0D\} & \{0E\} & \{09\} \\
 \{09\} & \{0B\} & \{0D\} & \{0E\}
 \end{bmatrix}$$

[0103] In Equation 4, four values, such as {09}, {0B}, {0D}, and {0E}, which are element values of the mixcolumn matrix, may be referred to as a mixcolumn multiplication value. When both an encryption operation and a decryption operation are integrated, seven values, such as {01}, {02}, {03}, {09}, {0B}, {0D}, and {0E}, may be referred to as the mixcolumn multiplication value.

[0104] The first to fourth encoders 213_11 to 213_14 may generate multiplication data by encoding a permutation value to represent a result of a mixcolumn multiplication operation on any one of a plurality of mixcolumn multiplication values. In this case, the first to fourth encoders 213_11 to 213_14 may generate multiplication data by encoding a permutation value to represent a result of the mixcolumn multiplication operation on some of the seven total mixcolumn multiplication values. Multiplication data not generated by the first to fourth encoders 213_11 through 213_14 may be generated by the first to third additional operation circuits 214_11 to 214_13.

[0105] The first to third additional operation circuits 214_11 to 214_13 may generate one or more pieces of multiplication data not generated by the first to fourth encoders 213_11 to 213_14 among a plurality of pieces of multiplication data based on the multiplication data generated by the first to fourth encoders 213_11 to 213_14. The first to third additional operation circuits 214_11 to 214_13 may generate one or more pieces of multiplication data not generated by the first to fourth encoders 213_11 to 213_14 by performing a logical operation (for example, an XOR operation) between the multiplication data generated by the first to fourth encoders 213_11 to 213_14.

[0106] In this case, the multiplication data generated by the first to fourth encoders 213_11 to 213_14 and the multiplication data generated by the first to third additional operation circuits 214_11 to 214_13 may be as illustrated in FIG. 8.

[0107] FIG. 8 is a table illustrating an example of a mixcolumn multiplication operation result that may be output through a plurality of encoders and a plurality of additional operation circuits in the sub security circuit of FIG. 7.

[0108] Referring to FIG. 8, the table shows whether multiplication data corresponding to a plurality of mixcolumn multiplication values is generated through an encoder or an additional operation circuit and a method of generating the multiplication data corresponding to the mixcolumn multiplication values by the additional operation circuit.

[0109] Referring to the table of FIG. 8, the first to fourth encoders 213_11 to 213_14 may generate multiplication data corresponding to mixcolumn multiplication values {01}, {02}, {0D}, and {09}. For example, the first encoder 213_11 may generate multiplication data corresponding to the mixcolumn multiplication value {01}, the second encoder 213_12 may generate multiplication data corresponding to the mixcolumn multiplication value {02}, the third encoder 213_13 may generate multiplication data corresponding to the mixcolumn multiplication value {0D}, and the fourth encoder 213_14 may generate multiplication data corresponding to the mixcolumn multiplication value {09}.

[0110] In addition, the first to third additional operation circuits 214_11 to 214_13 may generate multiplication data corresponding to the mixcolumn multiplication values {03}, {0E}, and {0B}. For example, the first additional operation circuit 214_11 may generate multiplication data corresponding to the mixcolumn multiplication value {03} by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {01} and the multiplication data corresponding to the mixcolumn multiplication value {02}. The second additional operation circuit 214_12 may generate multiplication data corresponding to the mixcolumn multiplication value {0E} by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {0D}, the multiplication data corresponding to the mixcolumn multiplication value {01}, and the multiplication data corresponding to the mixcolumn multiplication value {02}. The third additional operation circuit 214_13 may generate multiplication data corresponding to the mixcolumn multiplication value {0B} by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {09} and the multiplication data corresponding to the mixcolumn multiplication value {02}.

[0111] As described above, when the security circuit 200 including the sub security circuit 210_1 according to embodiments of FIGS. 7 and 8 is used, the number of encoders may be greatly reduced by using the first to third additional operation circuits 214_11 to 214_13, and thus, an increase in the total area of the security circuit 200 may be reduced.

[0112] FIG. 9 is a table illustrating a setting method of the mixcolumn multiplication operation result that may be output through a plurality of encoders and a plurality of additional operation circuits in the sub security circuit of FIG. 7.

[0113] Referring to FIG. 9, the table shows another setting method of a mix-column multiplication operation result that may be generated through the first to fourth encoders 213_11 to 213_14 and the first to third additional operation circuits 214_11 to 214_13 in the sub security circuit 210_1 according to an embodiment of FIG. 7.

[0114] Referring to the table illustrated in FIG. 9, the multiplication data corresponding to the mixcolumn multiplication

value {01} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {02} and the multiplication data corresponding to the mixcolumn multiplication value {03}.

[0115] The multiplication data corresponding to the mixcolumn multiplication value {09} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {02} and the multiplication data corresponding to the mixcolumn multiplication value {0B}.

[0116] The multiplication data corresponding to the mixcolumn multiplication value {0B} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {02} and the multiplication data corresponding to the mixcolumn multiplication value {09}.

[0117] The multiplication data corresponding to the mixcolumn multiplication value {0D} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {03} and the multiplication data corresponding to the mixcolumn multiplication value {0E}.

[0118] The multiplication data corresponding to the mixcolumn multiplication value {0E} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {03} and the multiplication data corresponding to the mixcolumn multiplication value {0D}.

[0119] In this case, in a first method, multiplication data corresponding to the mixcolumn multiplication values {02}, {03}, {09}, and {0D} may be generated by the first to fourth encoders 213_11 to 213_14, and multiplication data corresponding to the mixcolumn multiplication values {01}, {0B}, and {0E} may be generated by the first to third additional operation circuits 214_11 to 214_13.

[0120] In a second method, multiplication data corresponding to the mixcolumn multiplication values {02}, {03}, {09}, and {0E} may be generated by the first to fourth encoders 213_11 to 213_14, and multiplication data corresponding to the mixcolumn multiplication values {01}, {0B}, and {0D} may be generated by the first to third additional operation circuits 214_11 to 214_13.

[0121] In a third method, multiplication data corresponding to the mixcolumn multiplication values {02}, {03}, {0B}, and {0D} may be generated by the first to fourth encoders 213_11 to 213_14, and multiplication data corresponding to the mixcolumn multiplication values {01}, {09}, and {0E} may be generated by the first to third additional operation circuits 214_11 to 214_13.

[0122] In a fourth method, multiplication data corresponding to the mixcolumn multiplication values {02}, {03}, {0B}, and {0E} may be generated by the first to fourth encoders 213_11 to 213_14, and multiplication data corresponding to the mixcolumn multiplication values {01}, {09}, and {0D} may be generated by the first to third additional operation circuits 214_11 to 214_13.

[0123] When multiplication data generated by the first to fourth encoders 213_11 to 213_14 and the first to third additional operation circuits 214_11 to 214_13 is set by using the table illustrated in FIG. 9, output timing of the multiplication data generated by the first to third additional operation circuits 214_11 to 214_13 may be set identically to the first to third additional operation circuits 214_11 to 214_13 and may perform the same number of XOR operations.

[0124] FIG. 10 is a table illustrating an example in which a mixcolumn multiplication operation result may be generated by a configuration of a sub security circuit, according to an embodiment.

[0125] Referring to FIG. 10, a setting method of a mixcolumn multiplication operation result that may be generated by five encoders and seven additional operation circuits is illustrated, unlike the circuit illustrated in FIG. 7.

[0126] Referring to the table illustrated in FIG. 10, multiplication data corresponding to the mixcolumn multiplication value {01} may be obtained by performing an XOR operation between multiplication data corresponding to the mixcolumn multiplication value {02} and multiplication data corresponding to the mixcolumn multiplication value {03}.

[0127] The multiplication data corresponding to the mixcolumn multiplication value {02} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {01} and multiplication data corresponding to the mixcolumn multiplication value {03}.

[0128] The multiplication data corresponding to the mixcolumn multiplication value {03} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {01} and multiplication data corresponding to the mixcolumn multiplication value {02}.

[0129] Multiplication data corresponding to the mixcolumn multiplication value {09} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {01} and multiplication data corresponding to the mixcolumn multiplication value {08}, or by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {03} and multiplication data corresponding to the mixcolumn multiplication value {0A}.

[0130] Multiplication data corresponding to the mixcolumn multiplication value {0B} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {03} and the multiplication data corresponding to the mixcolumn multiplication value {08}, or by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {01} and the multiplication data corresponding to the mixcolumn multiplication value {0A}.

[0131] Multiplication data corresponding to the mixcolumn multiplication value {0D} may be obtained by performing

an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {01} and multiplication data corresponding to the mixcolumn multiplication value {0C}, or by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {02} and multiplication data corresponding to the mixcolumn multiplication value {0F}.

5 [0132] Multiplication data corresponding to the mixcolumn multiplication value {0E} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {02} and multiplication data corresponding to the mixcolumn multiplication value {0C}, or by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {01} and multiplication data corresponding to the mixcolumn multiplication value {0F}.

10 [0133] In this case, by utilizing five encoders, multiplication data corresponding to the mixcolumn multiplication values {01}, {02}, and {03} may be generated, any one of multiplication data corresponding to the mixcolumn multiplication values {08} and {0A} may be generated, any one of multiplication values {0C} and {0F} may be generated, and multiplication data corresponding to the mix column multiplication values {01}, {02}, {03}, {09}, {0B}, {0D}, and {0E} may be generated by seven additional operation circuits.

15 [0134] When multiplication data generated by five encoders and seven additional operation circuits is set by using the table illustrated in FIG. 10, output timing of all multiplication data may be set identically as all multiplication data is generated through an XOR operation of an additional operation circuit.

[0135] FIG. 11 is a table illustrating an example in which a mixcolumn multiplication operation result may be generated by a configuration of a sub security circuit, according to an embodiment.

20 [0136] Referring to FIG. 11, a setting method of a mixcolumn multiplication operation result that may be generated by five encoders and three additional operation circuits is illustrated, unlike the circuit illustrated in FIG. 7.

[0137] Referring to the table illustrated in FIG. 11, multiplication data corresponding to the mixcolumn multiplication value {01} may be obtained by performing an XOR operation between multiplication data corresponding to the mixcolumn multiplication value {08} and multiplication data corresponding to the mixcolumn multiplication value {09}, by performing an XOR operation between multiplication data corresponding to the mixcolumn multiplication value {0A} and multiplication data corresponding to the mixcolumn multiplication value {0B}, by performing an XOR operation between multiplication data corresponding to the mixcolumn multiplication value {0C} and multiplication data corresponding to the mixcolumn multiplication value {0D}, or by performing an XOR operation between multiplication data corresponding to the mixcolumn multiplication value {0E} and multiplication data corresponding to the mixcolumn multiplication value {0F}.

30 [0138] Multiplication data corresponding to the mixcolumn multiplication value {02} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {09} and the multiplication data corresponding to the mixcolumn multiplication value {0B}.

[0139] Multiplication data corresponding to the mixcolumn multiplication value {03} may be obtained by performing an XOR operation between the multiplication data corresponding to the mixcolumn multiplication value {0D} and the multiplication data corresponding to the mixcolumn multiplication value {0E}.

35 [0140] In this case, multiplication data corresponding to the mixcolumn multiplication values {08}, {09}, {0B}, {0D}, and {0E} may be generated by five encoders, and multiplication data corresponding to the mixcolumn multiplication values {01}, {02}, and {03} may be generated by three additional operation circuits.

40 [0141] When the multiplication data generated by the five encoders and the three additional operation circuits is set by using the table illustrated in FIG. 11, multiplication data used for an encryption operation is generated by three additional operation circuits, and multiplication data used for decryption operation is generated by five encoders, and accordingly, output timing between multiplication data used for encryption may be set identically and output timing between the multiplication data used for decryption may be set identically.

45 [0142] FIG. 12 is a block diagram illustrating a detailed configuration of a mixcolumn addition circuit and an example of data input and output to and from a security circuit according to an embodiment.

[0143] Referring to FIG. 12, in an embodiment, a mixcolumn addition circuit 300 may receive permutation data SuD. The permutation data SuD may include first to fourth sub permutation data SSuD1 to SSuD4, and each of the first to fourth sub permutation data SSuD1 to SSuD4 may include first to third multiplication data MD1 to MD3.

50 [0144] In an embodiment of FIG. 12, the mixcolumn addition circuit 300 may include first to fourth addition circuits 310_1 to 310_4.

[0145] In an embodiment of FIG. 12, the number of addition circuits (for example, the first to fourth addition circuits 310_1 to 310_4) may be equal to the number of pieces of sub shift data (for example, the first to fourth sub shift data SSD1 to SSD4).

55 [0146] The first addition circuit 310_1 may receive the first multiplication data MD1 of the first sub permutation data SSuD1, the third multiplication data MD3 of the second sub permutation data SSuD2, the second multiplication data MD2 of the third sub permutation data SSuD3, and the second multiplication data MD2 of the fourth sub permutation data SSuD4, and may sum the first to third multiplication data MD1 to MD3.

[0147] The second addition circuit 310_2 may receive the second multiplication data MD2 of the first sub permutation

data SSuD1, the first multiplication data MD1 of the second sub permutation data SSuD2, the third multiplication data MD3 of the third sub permutation data SSuD3, and the second multiplication data MD2 of the fourth sub permutation data SSuD4, and may sum the first to third multiplication data MD1 to MD3.

[0148] The third addition circuit 310_3 may receive the second multiplication data MD2 of the first sub permutation data SSuD1, the second multiplication data MD2 of the second sub permutation data SSuD2, the first multiplication data MD1 of the third sub permutation data SSuD3, and the third multiplication data MD3 of the fourth sub permutation data SSuD4, and may sum the first to third multiplication data MD1 to MD3.

[0149] The fourth addition circuit 310_4 may receive the third multiplication data MD3 of the first sub permutation data SSuD1, the second multiplication data MD2 of the second sub permutation data SSuD2, the second multiplication data MD2 of the third sub permutation data SSuD3, and the first multiplication data MD3 of the fourth sub permutation data SSuD4, and may sum the first to third multiplication data MD1 to MD3.

[0150] In addition, first mid data FMD may be generated by connecting summation results of the first to fourth addition circuits 310_1 to 310_4.

[0151] FIG. 13 is a flowchart illustrating an operating method of an encryption device, according to an embodiment.

[0152] Referring to FIG. 13, in operation S1310, the encryption device 1 may perform a round key addition operation. In this case, operation S1310 may correspond to a first round operation.

[0153] In operation S1320, the encryption device 1 may perform a shiftrow operation. In operation S1330, the encryption device 1 may perform a permutation operation. In operation S1340, the encryption device 1 may perform a round key addition operation.

[0154] In this case, operation S1320 to operation S1340 may correspond to an iterative round operation. Therefore, in operation S1350, whether a repeat number N exceeds a preset reference number (e.g., 9 in an embodiment of FIG. 13) may be determined. When it is determined that the repeat number N does not exceed the preset reference number (e.g., 9 in an embodiment of FIG. 13), the processing may return to operation S1320 to again perform the iterative round operation.

[0155] When it is determined that the repeat number N exceeds the preset reference number (e.g., 9 in an embodiment of FIG. 13), the iterative round operation may end and operation S1360 may be performed.

[0156] In operation S1360, the encryption device 1 may perform a shiftrow operation. In operation S1370, the encryption device 1 may perform a permutation operation. In operation S1380, the encryption device 1 may perform a mixcolumn multiplication elimination operation. In operation S1390, the encryption device 1 may perform a round key addition operation. In this case, operation S1360 to operation S1390 may correspond to a final round operation.

[0157] As a result of the final round operation, encrypted or decrypted final output data may be generated.

[0158] FIG. 14 is a block diagram illustrating a computing device according to an embodiment.

[0159] Referring to FIG. 14, the block diagram illustrates a computing device including electronic devices employing an encryption device according to an embodiment. In an embodiment, a computing device 1000 may include a processor device 1100, a working memory 1200, a storage device 1300, a user interface 1400, and a bus 1500.

[0160] For example, the computing device 1000 may be one of various electronic devices, such as a desktop computer, a laptop computer, a tablet computer, a workstation, a server, a digital television, a video game console, a smartphone, and a wearable device, but is not limited thereto.

[0161] The processor device 1100 may control all operations of the computing device 1000. The processor device 1100 may be configured to process various types of arithmetic operations and/or logical operations. To this end, the processor device 1100 may be implemented by a special-purpose logic circuit (for example, a field programmable gate array (FPGA), an application specific integrated circuit (ASIC), etc.) including one or more processor cores 1110. For example, the processor device 1100 may include a general-purpose processor, a dedicated processor, and/or an application processor.

[0162] For example, the processor device 1100 may execute an instruction set of program code by using the processor cores 1110. One or more caches 1130 may temporarily store data generated by executing an instruction set or data to be used for executing the instruction set.

[0163] The processor device 1100 may encrypt data output from the processor cores 1110 and/or caches 1130 by using an encryption device 1150. Furthermore, the processor device 1100 may decrypt data to be input to the processor cores 1110 and/or the caches 1130 by using the encryption device 1150.

[0164] The working memory 1200 may temporarily store data used for an operation of the computing device 1000. For example, the working memory 1200 may store data processed or to be processed by the processor device 1100 in one or more memories 1210. For example, the memories 1210 may include volatile memories, such as static random access memory (SRAM), dynamic RAM (DRAM), and synchronous DRAM (SDRAM). A memory controller 1230 may control the memories 1210 such that the memories 1210 store data or output the stored data.

[0165] The working memory 1200 may encrypt data to be stored in the memories 1210 by using an encryption device 1250. Furthermore, the working memory 1200 may decrypt data output from the memories 1210 by using the encryption device 1250.

[0166] The storage device 1300 may store data regardless of power supply. The storage device 1300 may store system data used to operate the computing device 1000 and/or user data for a user of the computing device 1000 in one or more nonvolatile memories 1310. For example, the nonvolatile memories 1310 may include at least one of nonvolatile memories, such as flash memory, phase-change RAM (PRAM), magneto-resistive RAM (MRAM), resistive RAM (ReRAM), and ferro-electric RAM (FRAM). A memory controller 1230 may control the nonvolatile memories 1310 such that the nonvolatile memories 1310 store data or output the stored data. For example, the storage device 1300 may include a storage medium, such as a solid state drive (SSD), a hard disk drive (HDD), a secure digital (SD) card, a multimedia card (MMC), etc.

[0167] The storage device 1300 may encrypt data to be stored in the nonvolatile memories 1310 by using an encryption device 1350. Furthermore, the storage device 1300 may decrypt data output from the nonvolatile memories 1310 by using the encryption device 1350.

[0168] The user interface 1400 may mediate communication between a user and the computing device 1000 under control of the processor device 1100. For example, the user interface 1400 may process an input from a keyboard, a mouse, a keypad, a button, a touch panel, a touch screen, a touch pad, a touch ball, a camera, a microphone, a gyroscope sensor, a vibration sensor, etc. Furthermore, the user interface 1400 may process an output to a display device, a speaker, or a motor.

[0169] The bus 1500 may provide a communication path between components of the computing device 1000. Components of the computing device 1000 may exchange data with each other based on a bus format of the bus 1500. For example, the bus format may include one or more of various communication protocols, such as peripheral component interconnect express (PCIe), nonvolatile memory express (NVMe), small computer system interface (SCSI), advanced technology attachment (ATA), serial ATA (SATA), parallel ATA (PATA), serial attached SCSI (SAS), and universal flash storage (UFS).

[0170] In this case, the encryption devices 1150, 1250, and 1350 illustrated in FIG. 14 may be configured by the encryption device 1 described above with reference to FIGS. 1 to 13.

[0171] By using the encryption device 1 and an operating method of the encryption device 1 described above, the security circuit 200 may generate permutation data by performing a permutation operation, which includes a mixcolumn multiplication operation, on shift data, and thus, a critical path may be reduced.

[0172] As is traditional in the field of the inventive concept, embodiments are described, and illustrated in the drawings, in terms of functional blocks, units and/or modules. Those skilled in the art will appreciate that these blocks, units and/or modules are physically implemented by electronic (or optical) circuits such as logic circuits, discrete components, microprocessors, hardwired circuits, memory elements, wiring connections, etc., which may be formed using semiconductor-based fabrication techniques or other manufacturing technologies. In the case of the blocks, units and/or modules being implemented by microprocessors or similar, they may be programmed using software (e.g., microcode) to perform various functions discussed herein and may optionally be driven by firmware and/or software. Alternatively, each block, unit and/or module may be implemented by dedicated hardware, or as a combination of dedicated hardware to perform some functions and a processor (e.g., one or more programmed microprocessors and associated circuitry) to perform other functions.

[0173] While the inventive concept has been particularly shown and described with reference to embodiments thereof, it will be understood that various changes in form and detail may be made therein without departing from the scope of the inventive concept as defined by the following claims.

Claims

45 1. An encryption device, comprising:

an encryption core circuit configured to generate output data by performing an encryption operation on input data; and

50 an encryption controller circuit configured to control an operation of the encryption core circuit, wherein the encryption core circuit comprises:

a shiftrow circuit configured to generate shift data by performing a shiftrow operation on the input data; a security circuit configured to generate permutation data by performing a permutation operation including a mixcolumn multiplication operation on the shift data;

55 a mixcolumn addition circuit configured to generate first mid data by performing a mixcolumn addition operation on the permutation data; and

a round key addition operation circuit configured to generate the output data by performing a round key addition operation on the first mid data.

2. The encryption device of claim 1, wherein the security circuit comprises a plurality of sub security circuits configured to receive any one of a plurality of pieces of sub shift data generated by dividing the shift data, and generate any one of a plurality of pieces of multiplication data included in sub permutation data by performing the permutation operation on the received sub shift data,

5

wherein the permutation operation includes the mixcolumn multiplication operation performed on any one of a plurality of mixcolumn multiplication values, and
the permutation data includes a plurality of pieces of the sub permutation data.

10 3. The encryption device of claim 2, wherein the sub shift data received by each of the plurality of sub security circuits is different from each other, or each of the plurality of sub security circuits performs the permutation operation on the mixcolumn multiplication values different from each other.

15 4. The encryption device of claim 3, wherein each of the plurality of sub security circuits comprises:

a decoder configured to decode the received sub shift data and output a decoded value;
a permutation circuit configured to output a selected permutation value based on the decoded value; and
an encoder configured to generate the multiplication data by encoding the permutation value to represent a result of the mixcolumn multiplication operation on any one of the plurality of mixcolumn multiplication values.

20

5. The encryption device of any preceding claim, wherein

the security circuit comprises a plurality of sub security circuits configured to receive any one of a plurality of pieces of sub shift data generated by dividing the shift data, and generate sub permutation data including a plurality of pieces of multiplication data by performing the permutation operation including the mixcolumn multiplication operation on the received sub shift data,

the permutation data includes a plurality of pieces of the sub permutation data,
each of the plurality of pieces of multiplication data is generated by performing the permutation operation on the sub shift data, and

30

the permutation operation includes the mixcolumn multiplication operation on any one of a plurality of mixcolumn multiplication values.

6. The encryption device of claim 5, wherein the sub shift data received by each of the plurality of sub security circuits is different from each other.

35

7. The encryption device of claim 6, wherein each of the plurality of sub security circuits comprises:

a decoder configured to decode the received sub shift data and output a decoded value;
a permutation circuit configured to output a selected permutation value based on the decoded value; and
a plurality of encoders configured to generate the multiplication data by encoding the permutation value to represent a result of the mixcolumn multiplication operation on any one of the plurality of mixcolumn multiplication values.

8. The encryption device of any of claims 6 to 7, wherein each of the plurality of sub security circuits comprises:

45

a decoder configured to decode a part of the received sub shift data and output a decoded value;
a permutation circuit configured to output a selected permutation value based on the decoded value;
a plurality of encoders configured to generate the multiplication data by encoding the permutation value to represent a result of the mixcolumn multiplication operation on any one of the plurality of mixcolumn multiplication values; and

one or more additional operation circuits configured to generate one or more pieces of multiplication data not generated by the plurality of encoders among the plurality of pieces of multiplication data, based on the multiplication data generated by the plurality of encoders.

55

9. The encryption device of any preceding claims, further comprising:

a mixcolumn multiplication elimination circuit configured to generate second mid data by performing a mixcolumn multiplication elimination operation on the permutation data,

wherein the round key addition operation circuit generates the output data by performing the round key addition operation on the second mid data.

10. An encryption device, comprising:

5 an encryption core circuit configured to generate output data by performing a plurality of round operations on input data; and
 10 an encryption controller circuit configured to control the encryption core circuit to sequentially perform the plurality of round operations including an initial round operation, an iterative round operation of a preset reference number of times, and a final round operation,
 15 wherein the encryption core circuit comprises a shiftrow circuit configured to generate shift data by performing a shiftrow operation on the input data, a security circuit configured to generate permutation data by performing a permutation operation including a mixcolumn multiplication operation on the shift data, a mixcolumn addition circuit configured to generate first mid data by performing a mixcolumn addition operation on the permutation data, and a round key addition operation circuit configured to generate the output data by performing a round key addition operation on the first mid data, and
 20 the iterative round operation includes the shiftrow operation, the permutation operation, the mixcolumn addition operation, and the round key addition operation.

20 11. The encryption device of claim 10, wherein

25 the security circuit comprises a plurality of sub security circuits configured to receive any one of a plurality of pieces of sub shift data generated by dividing the shift data, and generate any one of a plurality of pieces of multiplication data included in sub permutation data by performing the permutation operation on the received sub shift data,
 30 wherein the permutation operation includes the mixcolumn multiplication operation on any one of a plurality of mixcolumn multiplication values, and
 35 the permutation data includes a plurality of pieces of the sub permutation data.

30 12. The encryption device of claim 11, wherein the sub shift data received by each of the plurality of sub security circuits is different from each other, or each of the plurality of sub security circuits performs the permutation operation on the mixcolumn multiplication values different from each other,
 35 wherein the permutation operation includes the mixcolumn multiplication operation.

35 13. The encryption device of claim 12, wherein each of the plurality of sub security circuits comprises:

40 a decoder configured to decode the received sub shift data and output a decoded value;
 45 a permutation circuit configured to output a selected permutation value based on the decoded value; and
 50 an encoder configured to generate the multiplication data by encoding the permutation value to represent a result of the mixcolumn multiplication operation on any one of the plurality of mixcolumn multiplication values.

55 14. The encryption device of any of claims 10 to 13, wherein

45 the security circuit comprises a plurality of sub security circuits configured to receive any one of a plurality of pieces of sub shift data generated by dividing the shift data, and generate sub permutation data including a plurality of pieces of multiplication data by performing the permutation operation including the mixcolumn multiplication operation on the received sub shift data,
 50 the permutation data includes a plurality of pieces of the sub permutation data,
 55 each of the plurality of pieces of multiplication data is generated by performing the permutation operation on the sub shift data, and
 the permutation operation includes the mixcolumn multiplication operation on any one of a plurality of mixcolumn multiplication values.

55 15. The encryption device of claim 14, wherein the sub shift data received by each of the plurality of sub security circuits is different from each other.

FIG. 1

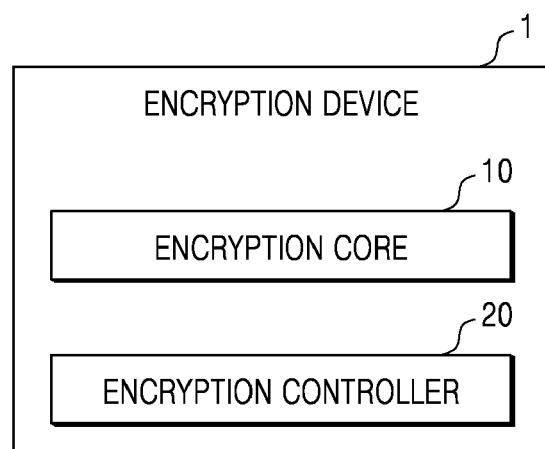


FIG. 2

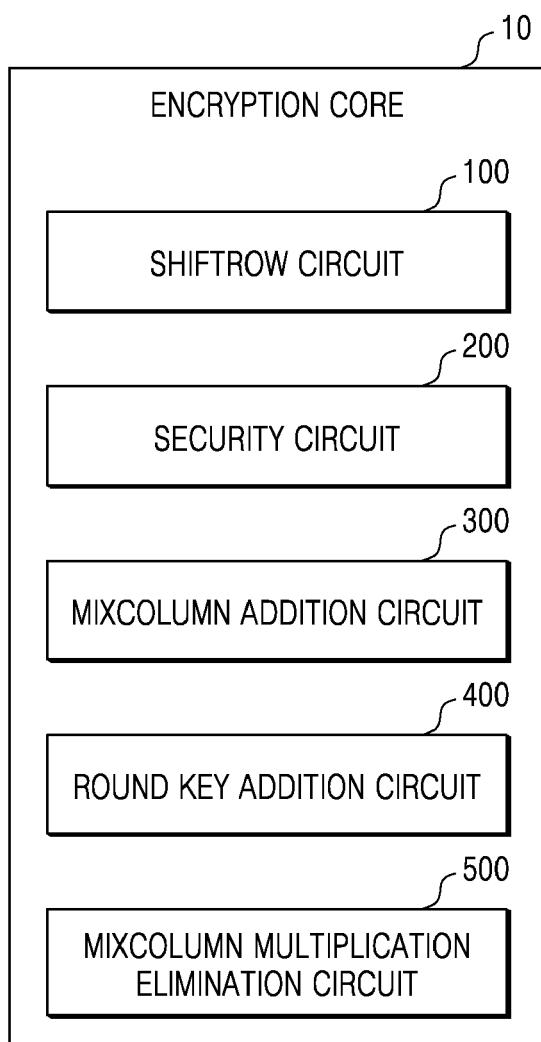


FIG. 3

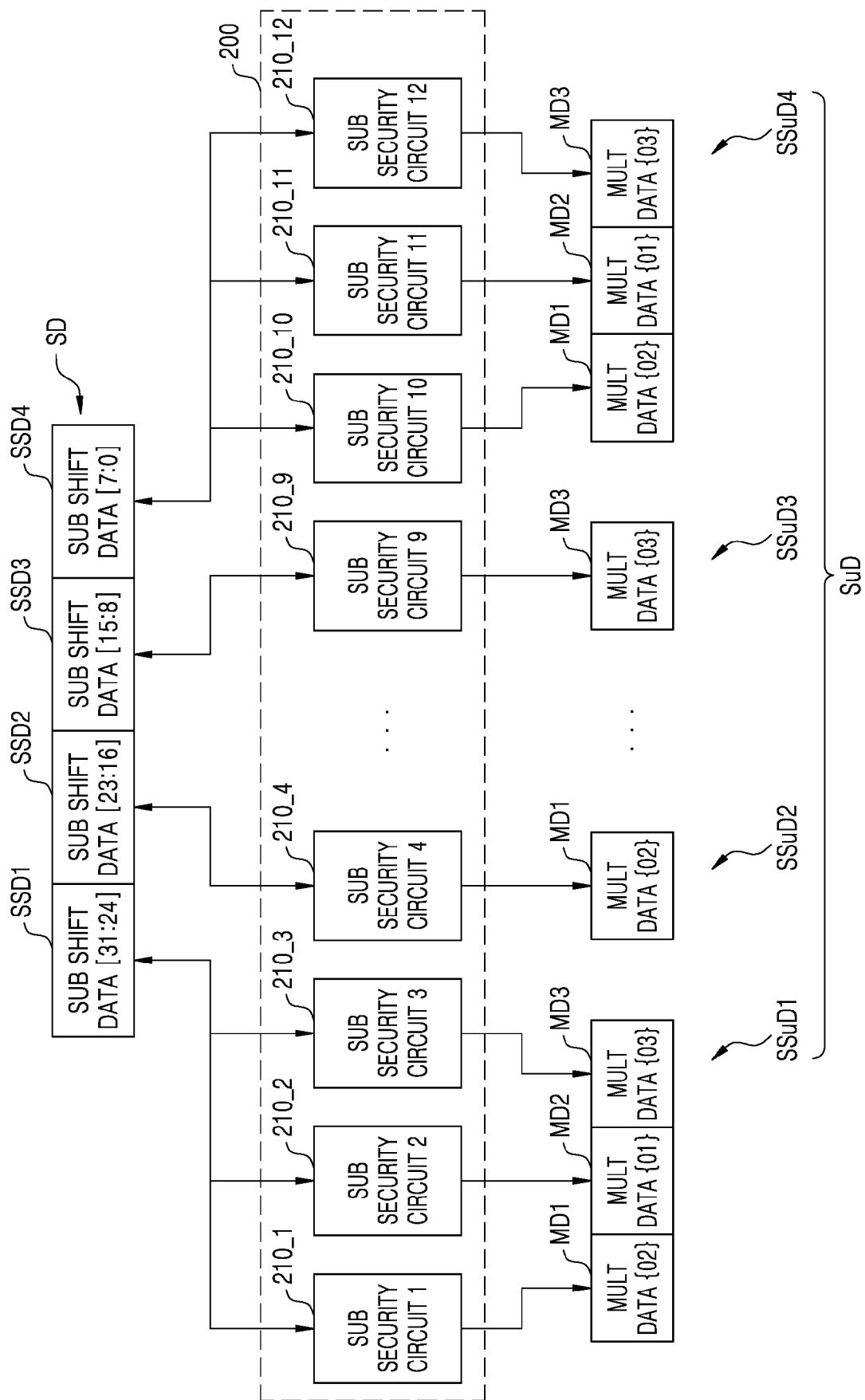


FIG. 4

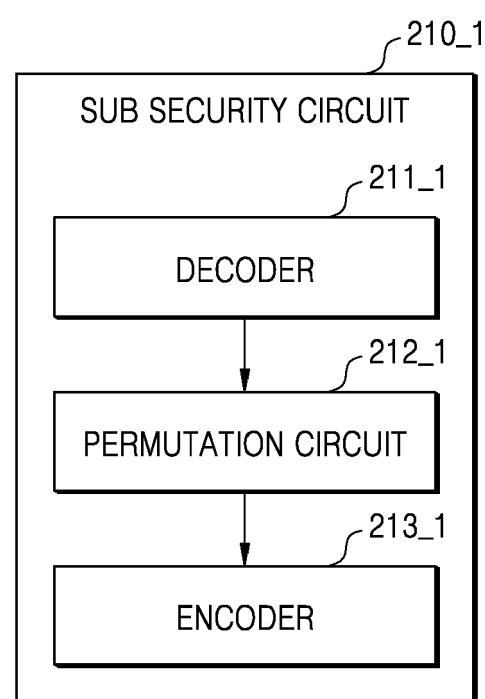


FIG. 5

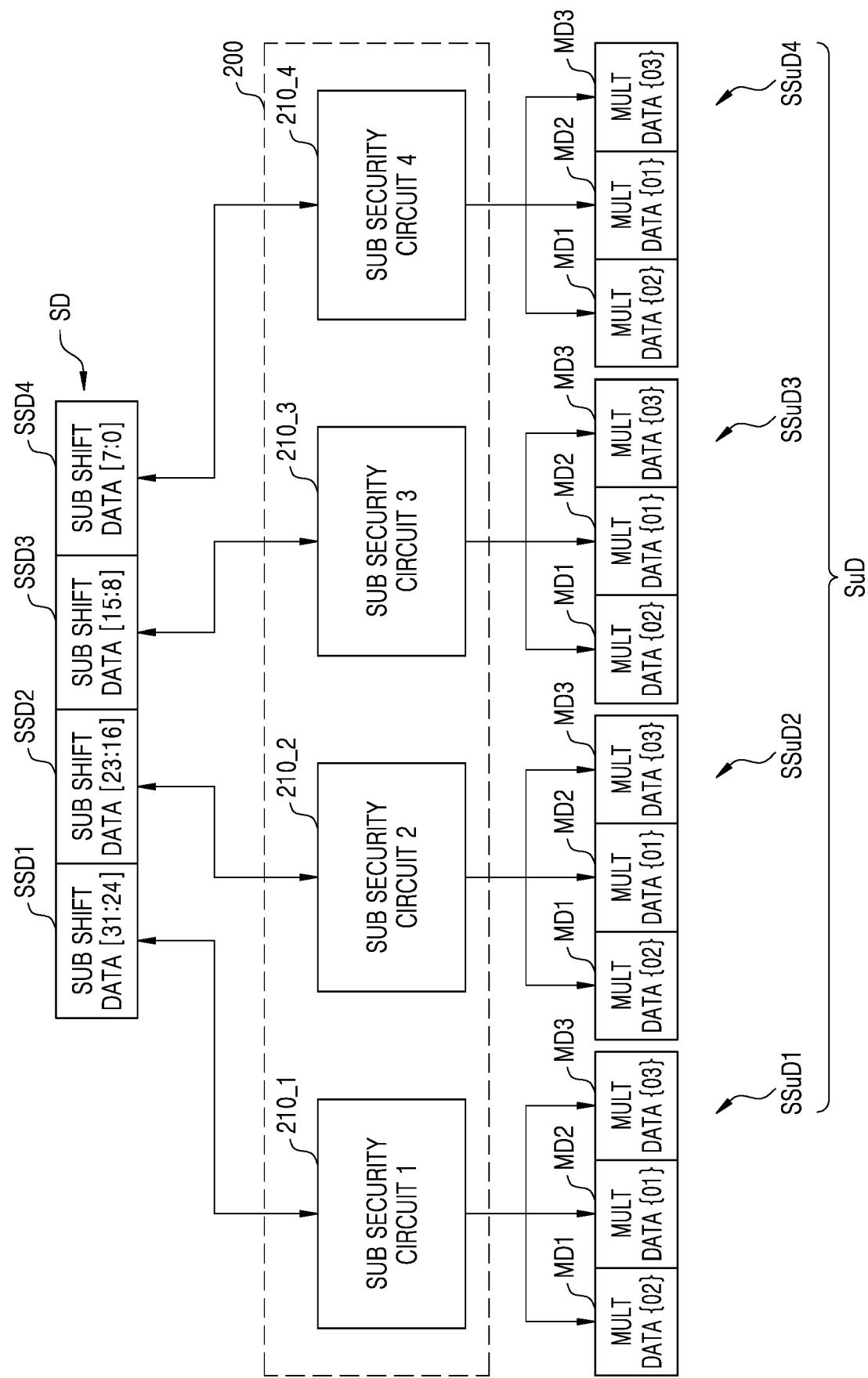


FIG. 6

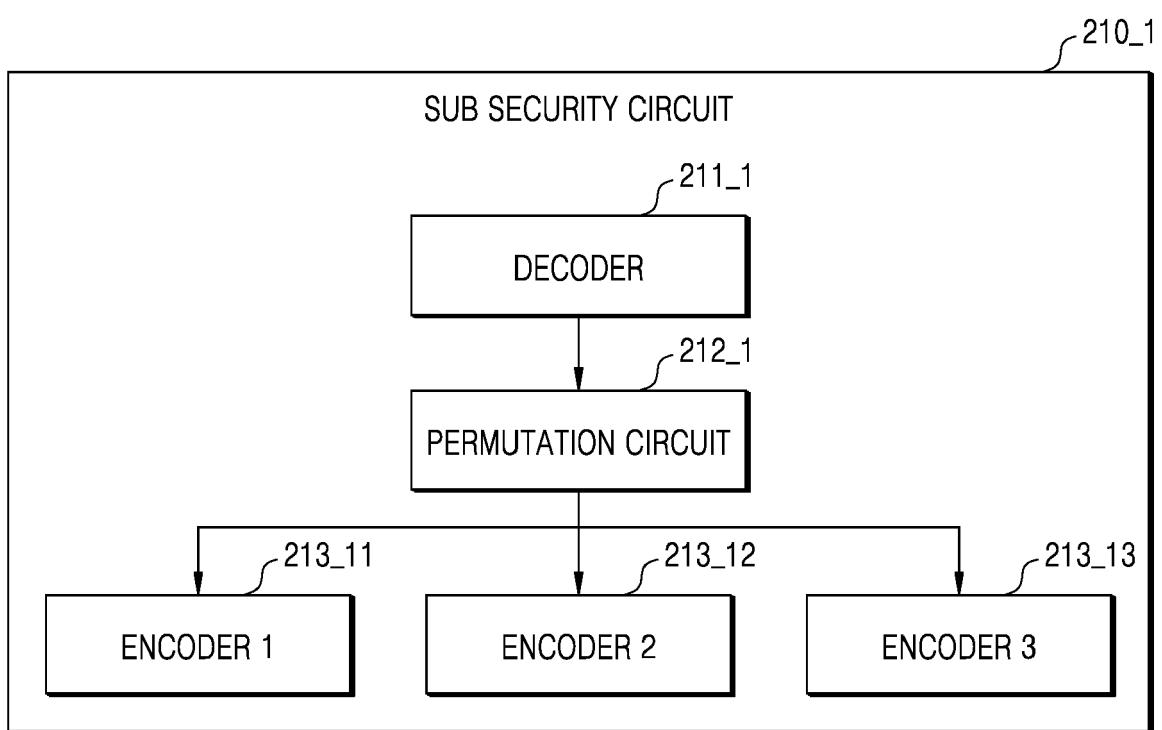


FIG. 7

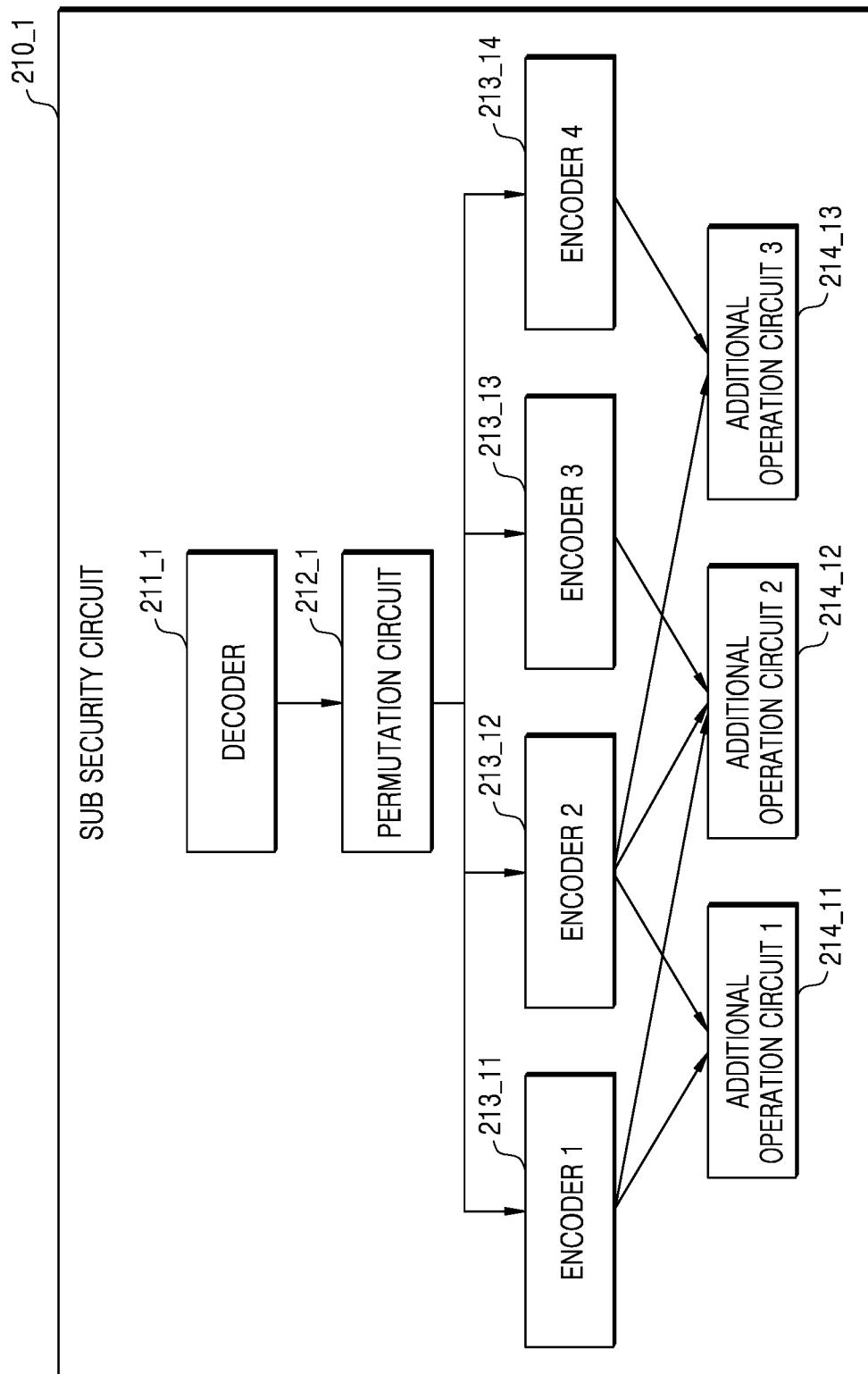


FIG. 8

MULTIPLICATION VALUE	BINARY	ENCODER	ADDITIONAL OPERATION CIRCUIT	COMBINATION
{01}	4'0001	○	X	-
{02}	4'0010	○	X	-
{03}	4'0011	X	○	{01}⊕{02}
{0E}	4'1110	X	○	{0D}⊕{01}⊕{02}
{0B}	4'1011	X	○	{09}⊕{02}
{0D}	4'1101	○	X	-
{09}	4'1001	○	X	-

FIG. 9

MULTIPLICATION VALUE	BINARY	COMBINATION
{01}	4'0001	{02} \oplus {03}
{02}	4'0010	-
{03}	4'0011	-
{09}	4'1001	{02} \oplus {0B}
{0B}	4'1011	{02} \oplus {09}
{0D}	4'1101	{03} \oplus {0E}
{0E}	4'1110	{03} \oplus {0D}

FIG. 10

MULTIPLICATION VALUE	BINARY	COMBINATION	
{01}	4'0001	{02}⊕{03}	
{02}	4'0010	{01}⊕{03}	
{03}	4'0011	{01}⊕{02}	
{08}	4'1000	-	
{09}	4'1001	{01}⊕{08}	{03}⊕{0A}
{0A}	4'1010	-	
{0B}	4'1011	{03}⊕{08}	{01}⊕{0A}
{0C}	4'1100	-	
{0D}	4'1101	{01}⊕{0C}	{02}⊕{0F}
{0E}	4'1110	{02}⊕{0C}	{01}⊕{0F}
{0F}	4'1111	-	

FIG. 11

MULTIPLICATION VALUE	BINARY	COMBINATION			
{01}	4'0001	{08} \oplus {09}	{0A} \oplus {0B}	{0C} \oplus {0D}	{0E} \oplus {0F}
{02}	4'0010	{09} \oplus {0B}	-	-	-
{03}	4'0011	{0D} \oplus {0E}	-	-	-

FIG. 12

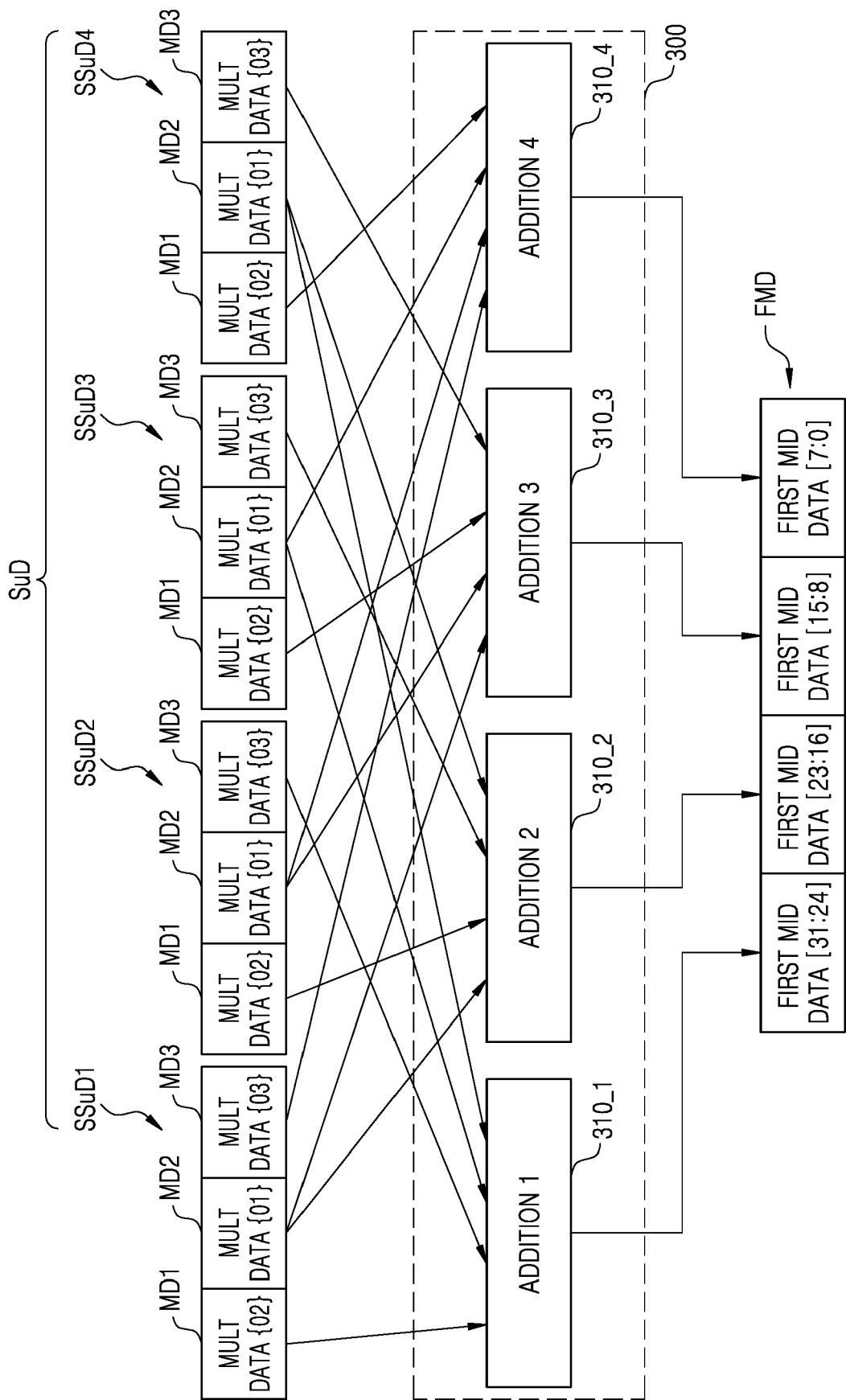


FIG. 13

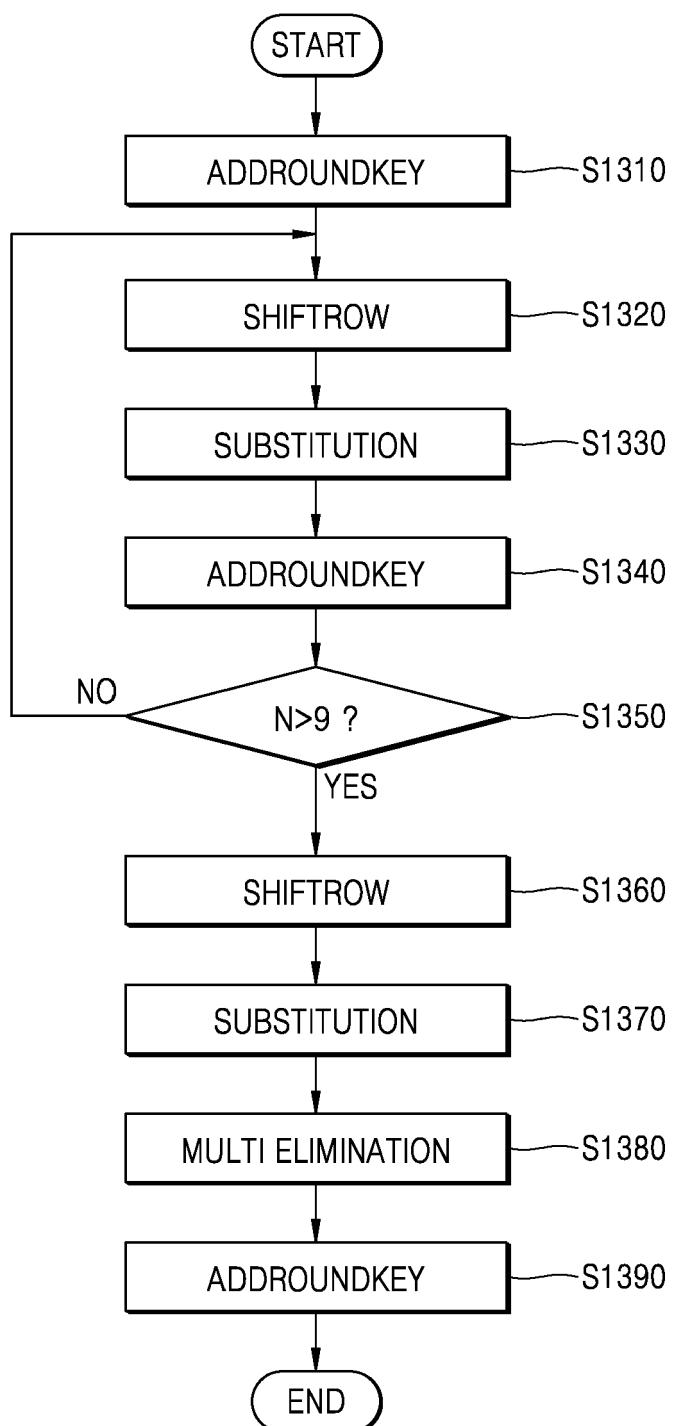
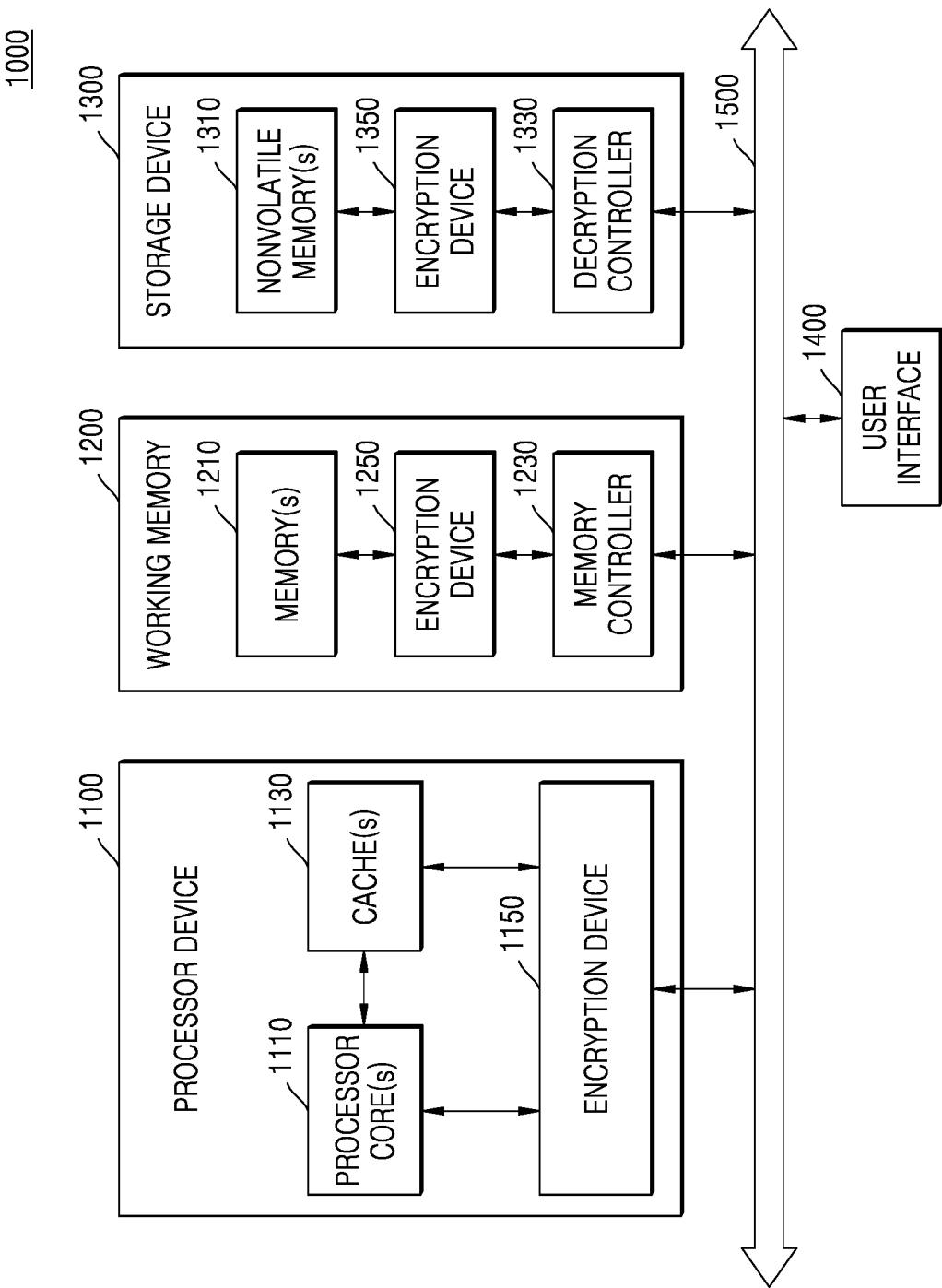


FIG. 14





EUROPEAN SEARCH REPORT

Application Number

EP 24 17 0357

5

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
10	X THE RIJNDAEL BLOCK CIPHER: "The Rijndael Block Cipher", IEEE DRAFT; PDFV5RHXENBDP, IEEE-SA, PISCATAWAY, NJ USA, vol. 802.15, 12 March 2009 (2009-03-12), pages 1-45, XP017765071, [retrieved on 2009-03-12] * sections 1, 4.1, 5.2.1 * -----	1-15	INV. H04L9/00 H04L9/06
15	X SRINIWAS SHASTRY P V ET AL: "Rolled architecture based implementation of AES using T-Box", CIRCUITS AND SYSTEMS (MWSCAS), 2012 IEEE 55TH INTERNATIONAL MIDWEST SYMPOSIUM ON, IEEE, 5 August 2012 (2012-08-05), pages 626-630, XP032231446, DOI: 10.1109/MWSCAS.2012.6292098 ISBN: 978-1-4673-2526-4 * section II * -----	1-15	
20	X FELDHOFER M ET AL: "AES implementation on a grain of sand Cryptographic algorithms and architectures for system-on-chip", 20051001, vol. 152, no. 1, 1 October 2005 (2005-10-01), pages 13-20, XP006025411, * section 2 * -----	1-15	
25			TECHNICAL FIELDS SEARCHED (IPC)
30			H04L
35			
40			
45			
50	1 The present search report has been drawn up for all claims		
55	1 Place of search Munich	1 Date of completion of the search 4 September 2024	1 Examiner Yamajako-Anzala, A
CATEGORY OF CITED DOCUMENTS			
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document			
T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			